CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-3
DISTRIBUTION: A, B, C, J, S

CJCSI 3213.01B
17 December 2003

JOINT OPERATIONS SECURITY

References: See Enclosure C.

1. Purpose. To provide CJCS policy and guidance for planning and executing operations security (OPSEC) in support of joint military operations.

2. Cancellation. CJCSI 3213.01A, 01 December 1997, "Joint Operations Security," is canceled.

3. Applicability. This instruction applies to the Joint Staff, combatant commands, Services, Defense agencies, and joint activities reporting to the Chairman of the Joint Chiefs of Staff.

4. Policy. Applicable organizations will conduct OPSEC activities in accordance with this instruction. See Enclosure A.

5. Definitions. See Glossary.

6. Responsibilities. See Enclosure B.

7. Summary of Changes

a. Is reorganized for reader clarity.

b. Is changed to reflect the integration of OPSEC with the other information operations (IO) core capabilities and emphasizes OPSEC as an integral part of full-spectrum IO.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page-http://www.dtic.mil/cjcs_directives. Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

9. Effective Date. This instruction is effective upon receipt.

Michael D. Maples

MICHAEL D. MAPLES
Major General, USA
Vice Director, Joint Staff

Enclosures:
A - Policy
B - Responsibilities
C - References
GL - Glossary

DISTRIBUTION

Distribution A, B, C, and J plus the following:

	Copies
Secretary of Defense (ASD C3I)	5
Director, Joint Interoperability Test Command	2
Commandant, Armed Forces Staff College	2
President, National Defense University	2
Director, Joint Warfighting Center	2
Director, Joint Command and Control Warfare Center	2
Director, Joint Warfare Analysis Center	2
Director, Joint COMSEC Monitoring Activity	2

(INTENTIONALLY BLANK)

ENCLOSURE A

POLICY

1. The Necessity for OPSEC

a. The events of 11 September 2001 served to enforce the immediate need to protect sensitive information; many nations and organizations are actively engaged in intelligence operations against the United States and its Armed Forces. This is especially true of terrorist organizations. Major sources of information for these groups include the media, the Internet, and observable activities of US Military Forces. Protection of critical information and friendly intentions is essential to mission accomplishment. Continual assessments of the OPSEC posture are needed to provide the very best effort to protect US forces and operations now and in the future.

b. The goal of OPSEC is to control information and observable actions about friendly force capabilities, limitations, and intentions so as to prevent or control their exploitation by an adversary. It is essential to maintain freedom of action for US Armed Forces. OPSEC measures are applicable across the entire range of military operations and are required:

(1) For any operation and/or activity, such as those that relate to the equipping, preparation, deployment, sustainment, or employment of the Armed Forces of the United States in time of peace, crisis and war that requires the maintenance of essential secrecy.

(2) For the protection of the information contained in Concept Plans, CONPLANs, OPLANs, OPORDs and supporting plans and orders.

(3) During force protection planning.

2. OPSEC and Information Operations (IO). OPSEC is integrated with and supports the other IO core capabilities to achieve the combatant commander's desired effects or prevent the enemy commander from achieving his. Full spectrum IO makes a potent contribution to effects-based operations across the full range of military operations. The OPSEC process is continuous and significantly contributes to the following IO functions:

a. Deter, discourage, dissuade, and direct an adversary, thereby disrupting the enemy's unity of command and purpose while preserving US unity of command.

b. Protect plans and misdirect the enemy forces, thereby allowing the US Military Services to mass its effect to maximum advantage while the adversary expends resources to little effect.

c. Control adversarial communications and networks and protect the US systems, thereby crippling the enemy's ability to direct and organize defense while preserving effective command and control of US forces.

3. OPSEC, Security and Counterintelligence

a. OPSEC is not security and is not intended to be a replacement for traditional security programs that were created to protect classified information. OPSEC is a process and was developed to deny adversaries publicly available indicators that are generally UNCLASSIFIED. OPSEC practices must be balanced against the Armed Forces responsibility to be accountable to the American people. The need to practice OPSEC should not be used as an excuse to deny non-critical information to the public.

b. To achieve surprise, military organizations must maintain essential secrecy. This is achieved through the combined efforts of:

(1) Security programs that deny classified information to adversaries. These traditional security programs include, but are not limited to, physical security, personnel security, signal security, computer security and information security.

(2) The OPSEC process to identify and control indicators of friendly actions and/or friendly information.

c. OPSEC and security programs are mutually supportive. Each must be effective for essential secrecy to be achieved. Planning to achieve this must address security program requirements and OPSEC measures simultaneously. Intelligence supports both OPSEC and security programs.

4. OPSEC and Operational Effectiveness

a. OPSEC contributes directly to operational effectiveness. A surprised adversary, or an adversary that has made poor decisions because of a lack of critical information, can be defeated more quickly and with fewer friendly losses than one who is prepared and well-informed.

b. To make a maximum contribution to operational effectiveness, there must be a balance between what must be denied to adversaries and what must be known to friendly personnel. Inadequate protection degrades this process by hindering the achievement of surprise. Excessive protection may impede effectiveness by interfering with required activities such as coordination, training or logistic support.

c. Proper use of the OPSEC process (reference c) will minimize the conflicts between operational and security requirements. It requires each operation be individually analyzed to determine its particular vulnerabilities and for the commander to determine what risks will be taken.

d. The OPSEC process recognizes that risk is inherent in all military activities. The determination of the appropriate level of protection versus operational needs requires an assessment of those risks. The use of the OPSEC process will assist commanders and force protection planners in determining the specific risk to information personnel, and facilities. Determining the balance between OPSEC measures and operational needs is the commander's decision.

5. The OPSEC Process. This process is applicable to all military operations and activities. Its use ensures that OPSEC measures address all significant aspects of the particular situation and are balanced against operational requirements. OPSEC is a continuous and iterative process. A detailed description is in reference c. The elements of the process are:

a. Identification of critical information.

b. Analysis of threats.

c. Analysis of vulnerabilities.

d. Assessment of risks.

e. Application of appropriate countermeasures.

6. OPSEC Programs. Commanders and heads of DOD components are required to establish and maintain formal OPSEC programs. The primary purpose of these programs is to support the commander by ensuring that the command or agency actively practices OPSEC to deny critical information to adversaries. Those organizations involved in and/or supporting joint activities must consider OPSEC in the development of programs. An OPSEC program provides for planning, training, education and evaluation. It promotes an understanding and awareness of OPSEC among all members of the command or agency. To be effective, an OPSEC program must have the following features:

a. Command Involvement. OPSEC is a command responsibility and success is based on the commander's active role in the program. The commander should provide OPSEC planning guidance early in the development process and be responsible for making key decisions. Those decisions include identifying the information and designating activities that must be protected. However, the commander may delegate the management of the program and its execution to subordinates.

b. Integration. The OPSEC process must be integrated into the planning and execution of all military operations and activities. As part of IO planning, OPSEC must be incorporated early in the conceptual phase of both deliberate and crisis action planning. Following command guidance is essential to OPSEC integration. Critical information must be identified for subordinate and supporting commands and specific guidance on the execution of OPSEC measures provided to them. Public Affairs and civil military operations are related activities, and these planners must be kept informed of that guidance and critical information for incorporation into their planning and operations.

c. Operational Orientation. OPSEC requires very close integration with the various security programs intended to protect classified information and information that is sensitive but unclassified. Management of a command or agency OPSEC program is not a security function. As one of the elements of IO, OPSEC is an operational function. When a commander delegates the authority for OPSEC planning and program management, that authority should be passed to the operations officer (or equivalent position).

d. Training and Education. Training and education programs ensure that all personnel understand the OPSEC process, know the command's critical information and are aware of any intelligence threats to the command. OPSEC training programs should be mission-related and tailored to the individual's specific duties. All personnel must understand that the practice of OPSEC is both an individual and a command responsibility. NSA, through the Interagency OPSEC Support Staff (IOSS), conducts interagency OPSEC training (reference a). Two courses are applicable to combatant command, Service and DOD agency personnel:

(1) OPSE-2380. Teaches the fundamentals. Students learn the principles and the use of the five step OPSEC process for planning activities, operations and programs. The focus is on applying those principles in the workplace. OPSE-2380 training is applicable for commanders and all staff personnel.

(2) OPSE-2390. This course provides detailed instruction on the development and implementation of an OPSEC program. It is specifically designed for OPSEC program managers.

e. Annual Reviews. Annual internal reviews to determine the status of a command's OPSEC program are necessary to program improvement. Additionally, the extent to which DOD components maintain OPSEC programs should be a key area for evaluation during visits by inspectors general.

f. Evaluation of OPSEC Programs. Evaluation of the organization's program can be made by: inspecting it for compliance of regulations; by assessing the program for completeness; and by surveying the organization's OPSEC profile. In any case, each can be undertaken by members of the organization or by personnel external to the organization. Red and Blue Teams' evaluations provide insight into the commands OPSEC training program and allow commanders to focus on training weaknesses.

(1) OPSEC Inspections. Inspections normally look for compliance to regulations and SOPs. Commanders may choose to conduct internal inspections or external inspections (e.g., inspectors general). Inspections tend to be narrowly focused on compliance to written program requirements, and while a program may look good on paper, it may be ineffective.

(2) OPSEC Assessments. This term refers to an evaluation of the organization's compliance with OPSEC plans and programs and appraises the OPSEC posture. Commanders may choose to conduct assessments with a small team of experts from within the organization. This team should be composed of the OPSEC Program Manager, a representative from each security discipline and at least one representative from the operations and intelligence staff sections.

(3) OPSEC Surveys. A survey is an evaluation of the organization's ability to apply the OPSEC methodology to operations. This evaluation should focus on the agency's ability to adequately protect critical information from adversary intelligence exploitation during planning, preparation, execution and post-execution phases of any operation or program.

g. Coordination. OPSEC must be coordinated and synchronized with other IO core capabilities to achieve the commanders' desired intent. Other IO capabilities are less effective if the adversary is alerted. Cross-command and interagency support and coordination during all phases of the OPSEC process enhance program effectiveness. Coordination is particularly vital for activities such as strategic C2 and counterdrug operations that involve multiple commands and agencies. Because of the importance of coalition warfare to US national strategy, allies should be encouraged to adopt US joint OPSEC concepts. Close coordination is required with intelligence organizations to identify potential adversaries and their intelligence collection capabilities and to determine how well critical information is being denied to adversaries.

7. OPSEC Program Officers

a. The OPSEC program officer is responsible for advising the commander on all OPSEC-related matters and for the day-to-day management of the organization's program. The position should be located within the operations element of the organization or on the commander's staff and requires a security clearance appropriate to the mission and functions of the organization.

b. Military planners responsible for base plans in support of operations and other activities are the best individuals to conduct OPSEC planning and execution. The role of the OPSEC program officer is to facilitate OPSEC within the IO plan. The program officer must participate in the planning process from the earliest stages to assist in the development of IO objectives and to assist the IO planners in the development and integration of OPSEC measures into the plans. Using the OPSEC process, the IO planners, assisted by the program officer and following the commander's guidance, can determine the OPSEC requirements for an activity. The development of the OPSEC portion of a plan is the responsibility of the OPSEC program officer and the IO planners. In circumstances involving particularly complex operations or operations requiring extraordinary security, it may be necessary to create dedicated OPSEC planning groups.

c. OPSEC program officers for the combatant commands, Defense agencies and Services should attend the interagency OPSEC training courses offered by NSA. Other training courses should be attended when possible.

d. The major duties of an OPSEC program officer may include:

(1) Advising the commander on OPSEC matters.

(2) Recommending OPSEC guidance to the commander.

(3) Coordinating the development of the OPSEC-related portions of operations plans and orders.

(4) Participating in IO planning.

(5) Developing and maintaining the organization's OPSEC program to include writing the organization's policy and guidance documents.

(6) Conducting organizational OPSEC education and awareness training to include coordinating attendance of personnel, especially operations and logistics planners, at IOSS-conducted interagency OPSEC training.

(7) Coordinating the conduct of OPSEC evaluations.

(8) Conducting the organization's annual OPSEC review.

(9) Developing and maintaining an organizational OPSEC lessons learned data base.

(10) Coordinating appropriate intelligence and counterintelligence support.

(11) Advising organizational inspectors general on the OPSEC program.

(12) Coordinating with security programs officers.

(13) Coordinating with IO supporting and related capabilities.

(INTENTIONALLY BLANK)

ENCLOSURE B

RESPONSIBILITIES

1. Chairman of the Joint Chiefs of Staff

a. Advises the Secretary of Defense concerning OPSEC support to the combatant commands.

b. Provides OPSEC policy, doctrine, joint tactics, techniques and procedures.

c. Provides procedures for OPSEC planning in JOPES.

d. Ensures that appropriate OPSEC measures are implemented during CJCS exercises.

2. Director for Operations (J-3), Joint Staff

a. Executes primary Joint Staff responsibility for OPSEC.

b. Designates OPSEC staff positions for the Joint Staff.

c. Maintains an OPSEC lessons-learned data base as a subset of the Joint Universal Lessons Learned System data base maintained by the Director for Operational Plans and Interoperability (J-7), Joint Staff, to support OPSEC planning and training by the Joint Staff, Services, combatant commands and Defense agencies.

d. Establishes and maintains an OPSEC orientation program for Joint Staff officers, enlisted personnel and civilians.

e. Assists commands and joint agencies in arranging and scheduling IOSS participation in OPSEC surveys.

f. Coordinates with J-7, Joint Staff, to ensure that OPSEC is adequately addressed in OPLANs and CONPLANs.

g. Assigns an OPSEC liaison officer (LO) during periods of crisis and during CJCS exercises to assist all Joint Staff elements in integrating OPSEC into crisis management planning efforts. The OPSEC LO will also serve as a point of contact to coordinate OPSEC issues with the combatant commands, Defense agencies and Services.

h. Establishes OPSEC Executive Groups (OEG), as necessary, composed of members of the Joint Staff, Services and appropriate agencies, to address specific OPSEC issues related to OPSEC programs that involve multiple commands or agencies.

3. Service Chiefs

a. Provide Service OPSEC policy, doctrine and planning procedures consistent with joint OPSEC policy, doctrine and guidance.

b. Provide for OPSEC-related training of appropriate Service members.

c. Designate an OPSEC program officer in the operations element of the Service headquarters.

d. Designate representatives to Joint Staff OEGs, when required.

e. Provide OPSEC lessons learned to the J-3 and J-7, Joint Staff, for inclusion in the OPSEC lessons-learned data base.

f. Provide to J-3, Joint Staff, J-39/DDIO/TSB, copies of all current Service OPSEC program directives and/or policy implementation documents.

4. Commanders of Combatant Commands

a. Provide OPSEC guidance for all command operations, exercises, and other joint activities of the command.

b. Conduct OPSEC planning in accordance with references a through m.

c. Provide OPSEC guidance and identify command critical information to all supporting combatant commands, Services other agencies and appropriate public affairs offices.

d. Coordinate OPSEC measures and their execution with USSTRATCOM and other commands and agencies of those activities that cross command boundaries. Report any unresolved issues to J-3, Joint Staff, J-39/DDIO for assistance.

e. Plan for and execute OPSEC measures in support of assigned missions during peacetime, crisis and war.

f. Conduct OPSEC surveys in support of command operations.

g. Designate an OPSEC program officer in the J-3/IO element of the command headquarters.

h. Conduct annual OPSEC program reviews. Identify areas requiring additional CJCS guidance, assistance, or clarification to the J-3, Joint Staff, J-39.

i. Provide OPSEC lessons learned to the J-3 and J-7, Joint Staff, for inclusion in the joint OPSEC lessons-learned database.

j. Provide to J-3, Joint Staff, J-39, copies of all current command OPSEC program directives and/or policy implementation documents.

5. Director, Defense Intelligence Agency

a. Establishes and maintain an OPSEC training program for DIA civilian and military personnel and attendees at the Defense Intelligence College.

b. Designates an agency joint OPSEC program officer.

c. Designates representatives to Joint Staff OEGs, as required.

d. Identifies, reviews, and validates DIA and other DOD threat assessment documents for Joint Staff use.

e. Conducts analysis of the foreign intelligence collection threat for required nations and organizations for use in OPSEC planning and for monitoring the effectiveness of implemented OPSEC measures. Provides results to the Chairman of the Joint Chiefs of Staff, combatant commanders, Chiefs of the Services, and heads of Defense agencies.

6. Director, National Security Agency. In accordance with references a and b:

a. Assists DOD components in establishing OPSEC programs, as requested.

b. Provides interagency OPSEC training courses.

c. Designates representatives to Joint Staff OEGs, as required.

d. Collaborates with the heads of the DOD components by providing:

(1) Technical OPSEC survey support to DOD components to assist them in identifying their OPSEC vulnerabilities.

(2) When requested, recommendations relating to doctrine, methods and procedures to minimize those vulnerabilities.

(3) Communications and computer security support for OPSEC surveys.

(4) SIGINT support for OPSEC threat development.

7. Heads of Other Defense Agencies and Joint Activities

a. Designate an agency joint OPSEC program officer.

b. Coordinate OPSEC programs and activities with commands and other agencies, as required.

c. Provide representatives to OEGs, as required.

ENCLOSURE C

REFERENCES

a. National Security Decision Directive Number 298, 22 January 1988, “National Operations Security Program.”

b. DOD Directive 5205.2, 29 November 1999, “DoD Operations Security Program.”

c. Joint Pub 3-54, 24 January 1997, “Joint Doctrine for Operations Security.”

d. Joint Pub 1, 14 November 2000, “Joint Warfare of the Armed Forces of the United States.”

e. Joint Pub 1-02, 12 April 2001, updated through 5 September 2003, “Department of Defense Dictionary of Military and Associated Terms.”

f. Joint Pub 3-13.1, 7 February 1996, “Joint Doctrine for Command and Control Warfare (C2W).”

g. Joint Pub 1-01, 5 July 2000, “Joint Doctrine Development System.”

h. Joint Pub 2-01.2, 7 May 2002, “Joint Doctrine and Tactics, Techniques, and Procedures for Counterintelligence Support to Operations.”

i. Joint Pub 5-0, 13 April 1995 “Doctrine for Planning Joint Operations.”

j. CJCSM 3122.03, 31 December 1999, CH-1 6 September 2000, JOPES, Volume II, “Planning Formats and Guidance.”

k. CJCSI 3210.01A, 6 November 1998, “Information Operations Policy (U)”

l. CJCS Handbook 5260, 1 January 1997, “Commander’s Handbook for Antiterrorism Readiness.”

m. Information Operations Roadmap, 30 October 2003.

(INTENTIONALLY BLANK)

GLOSSARY

counterintelligence (CI). Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 1-02)

critical information. Information about friendly activities, intentions, capabilities, or limitations that an adversary needs in order to gain a military, political, diplomatic, or technological advantage.

indicators. In OPSEC usage, friendly, detectable actions and open-source information (usually unclassified) that can be interpreted or pieced together by an adversary to derive critical information.

information operations (IO). The integrated employment of the core capabilities of Electronic Warfare, Computer Network Operations, Psychological Operations, Military Deception and Operations Security, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making while protecting our own.

operations security (OPSEC). A process of identifying critical information and, subsequently, analyzing friendly actions attendant to military operations and other activities to:

- Identify those actions that can be observed by adversary intelligence systems.

- Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

- Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

(INTENTIONALLY BLANK)